|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **㈜아이티아이즈**  **클라우드컴퓨팅서비스를**  **제공하기 위한**  **운영문서로서 검토되고**  **승인됨** | **구분** | **직위** | **성명** | **일자** | **서명** |
| 승인 | 클라우드서비스  센터장 | 경대진 |  |  |
| 검토 | 클라우드서비스  지원팀장 | 박수용 |  |  |
| 작성 | 담당자 | 김선환 |  |  |

모의훈련 세부 수행계획서

2022.04.29



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 재•개정 이력사항 | | | | |
| 번호 | 날짜 | 쪽 | 내용 | 담당자 |
| 1 | 2022.02.16 | 19 | 모늬훈련 세부 계획서 | 담당자 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

본 문서는 ㈜아이티아이스 클라우드 서비스 제공을 위해서 컨설팅, 마이그레이션, 매니지드, XaaS 서비스 등을 대상으로 작성함.

Ⅰ. 모의 훈련 개요

1. 모의훈련 대상

❍ 훈련 대상 : IaaS 인증사업자 3개 총 3개 사업자

- IaaS 인증사업자 자원 고갈 공격, SaaS 인증사업자 APT 이메일 훈련

|  |  |  |
| --- | --- | --- |
| 구분 | 훈련대상 | 훈련 사항 |
| IaaS | KT, NHN, 네이버 클라우드 | ICMP / GET / DNS / UDP Flooding |
| 통신량 한계 초과 / 접속처리 한계 초과 공격 |
| Slowloris / Cache-Control / HTTP Post Attck 홈페이지부하 가중 및 복합 공격 DNS Query Flooding (신청사업자) |
| IaaS(도상 훈련) | KT, NHN, 네이버 클라우드 | 훈련상황 : DDoS 공격으로 클라우드 IaaS 인증 서비스 10분 간 단절로 인한 사업자 침해사고 대응능력 확인 |

2. 모의훈련 일정(안)

- 훈련 대상 사업자별 1일씩 진행 총 6일 소요 예정(인증사업자와 협의)

※예상 일정 : 9월 30일(월) ~ 10월 2일(수) / 10월 7일(월) ~ 8일(화), 10일(목)

3. 모의훈련 전체 예상 소요 시간

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 내용 | 소용시간 | 훈련시작 | 종료시간 | 비고 |
| DDoS 모의훈련  (IaaS) | 공격 유형에 따른 모의훈련 진행 | 약 4시간 | 10:00 | 14:40 | 점심시간 1시간 제외 |
| 도상 훈련( IaaS) | 침해대응 절차에 따른 도상훈련 진행 | 2시간 | 15:00 | 17:00 | 훈련 결과보고서 |
| 훈련 평가 | 침해대응 절차서 및 훈련 결과 보고서를 참고하여 훈련 평가 | 1시간 | 17:00 | 18:00 | 훈련 평가지표 |

Ⅱ. 훈련 세부 내용

1. DDoS 모의훈련 구성 방안

❍ 내부 수행 : 상단 Router에서 내부 보안 장비를 거쳐 타켓 서버(홈페이지 또는 테스트 서버) 공격

❍ 외부 수행 : 외부(수행사내)에서 인터넷을 통해 인증 사업자 내부 보안 장비를 거쳐 타켓 서버(홈페이지 또는 테스트 서버) 공격

|  |  |
| --- | --- |
| 구분 | 구성도 |
| 내부수행 :  KT |  |
| 외부수행 :  KT, NHN, 네이버 클라우드 |  |